TS226 - Codes correcteurs
année 2019/2020

Romain Tajan

Exercice 1 -

Soit la matrice G à coefficients dans $\mathbb{F}_2$ donnée par

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Question 1. Vérifier que G est la matrice génératrice d'un code linéaire dont on précisera la longueur, la dimension ainsi que le rendement de code.

Question 2. Mettre le code sous forme systématique et trouver tous les mots de codes.

Question 3. Trouver une matrice de parité H, et en déduire les équations de parité du code.

Question 4. Déterminer la distance minimale de ce code ainsi que son spectre de poids.

Question 5. Combien d'erreurs peut-il détecter ?

Question 6. Combien d'erreurs peut-il corriger, par décodage au plus proche voisin ? Le code est-il MDS, parfait ?

Question 7. Après transmission dans un canal binaire symétrique, on reçoit la séquence $[1,0,0,1,0,1,0,1,0,1,0,1,0,0,1,0,0,0]$. Quelles sont les conditions sur les erreurs présentes dans la séquence, pour garantir un décodage parfait ? En supposant ces conditions satisfaites, effectuer le décodage de la séquence, à l'aide de la méthode du syndrome.

Exercice 2 - Construction de Plotkin

Soient $\mathcal{C}_1 = [n, k_1, d_1]$ et $\mathcal{C}_2 = [n, k_2, d_2]$ deux codes linéaires binaires de même longueur n. La méthode de Plotkin permet de construire un nouveau code $\mathcal{C}$ à partir de deux codes linéaires $\mathcal{C}_1$ et $\mathcal{C}_2$, donné par

$$\mathcal{C} = \{(\mathbf{c_1}; \mathbf{c_1} + \mathbf{c_2}) : \mathbf{c_1} \in \mathcal{C}_1; \mathbf{c_2} \in \mathcal{C}_2\}$$

Question 1. Montrer que le code de Plotkin est linéaire, et donner ses longueur, dimension et rendement.

Question 2. En notant, G_1 et G_2 les matrices génératrices de $\mathcal{C}_1$ et $\mathcal{C}_2$, donner une matrice génératrice G de $\mathcal{C}$.

Question 3. Montrer que $d_{min}(\mathcal{C}) \leq \min\{2d_1, d_2\}$

Question 4. Montrer que pour tout $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$,

$$w_H(\mathbf{x}+\mathbf{y}) = w_H(\mathbf{x}) + w_H(\mathbf{y}) - 2w_H(\mathbf{x} \odot \mathbf{y}),$$

où $\odot$ représente le produit de Hadamard (produit terme à terme).

Question 5. Déduire de la question précédente que pour $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_1+\mathbf{c}_2) \in \mathcal{C}$, $w_H(\mathbf{c}) \geq w_H(\mathbf{c}_2)$.

Question 6. Déduire finalement que $d_{min}(\mathcal{C}) = \min\{2d_1, d_2\}$.

Exercice 3 - Extension du code de parité

Considérons un message à transmettre de 4 bits $\mathbf{u} = (u_0, \ldots, u_3)$. On ajoute au message 5 bits $\mathbf{p} = (p_0, \ldots, p_4)$ pour former le mot de code $\mathbf{c} = (p_0, \ldots, p_4, u_0, \ldots, u_3)$ tels que la matrice

$$\begin{bmatrix} u_0 & u_2 & p_0 \\ u_1 & u_3 & p_1 \\ p_2 & p_3 & p_4 \end{bmatrix}$$

aient des lignes et colonnes de somme nulle.

Question 1. Vérifier que le code défini est bien linéaire. Quelles sont sa longueur n et sa dimension k ?

Question 2. Donner une matrice génératrice de ce code.

Question 3. Quelle est la distance minimale ? Combien d'erreur peut-il corriger/détecter ?

Exercice 4 - Sur le code à répétitions et le code de parité

Soit $\mathcal{C}$ le code à n répétitions encodant des messages de $k = 1$ bit.

Question 1. Énumérer tous les mots de codes possibles.

Question 2. Quelle est la distance minimale de ce code, son spectre des poids.

Question 3. Ce code est-il MDS ?

Question 4. Donner une matrice génératrice G pour $\mathcal{C}$ sous la forme systématique.

Question 5. Déduire de la question précédente une matrice de parité H pour $\mathcal{C}$.

Question 6. Montrer que le code de parité est le code dual du code de répétition.

Exercice 5 - Borne de Plotkin

Soit $\mathcal{C} = [n, k, d]$ de matrice génératrice G.

Question 1. Dans le cas d'un message $\mathbf{u} = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_2^k$, l'équation vérifiée par le j-ème symbole c_j du mot de code $c = (c_0, \ldots, c_{n-1})$ associé, est donnée par

$$c_j = \sum_{i=0}^{k-1} u_i G_{i,j}$$

En supposant la j-ième colonne de G non nulle, montrer qu'il y a exactement 2^{k-1} mots de code de $\mathcal{C}$ dont la j-ème composante est non nulle.

Question 2. Déduire une borne supérieure sur la valeur de la somme des poids de tous les mots du code $\mathcal{C}$, i.e. un majorant de $\sum_{\mathbf{c}\in\mathcal{C}} w_H(\mathbf{c})$.

Question 3. Déduire alors la borne de Plotkin :

$$d \leq \frac{n2^{k-1}}{2^k - 1}$$

Exercice 6 - Borne de Hamming

Soit $\mathcal{C}$ un code (M, n) $q - aire$ construit pour un canal sans mémoire tel que $\mathcal{X} = \mathcal{Y} = \{0, 1, \cdots, q-1\}$. On souhaite démontrer la borne de Hamming donnée par l'inégalité suivante :

$$M \leq \frac{q^n}{\sum_{j=0}^{t} \binom{n}{r}(q-1)^j}, \text{ où } t = \lfloor \frac{d-1}{2} \rfloor$$

Un code de paramètres n, M et d vérifiant l'égalité est appelé un **code parfait**.

Question 1. Soit $\mathbf{x} \in \mathcal{X}^n$, on note $V(\mathbf{x}, r) = |\{\mathbf{y} \in \mathcal{X} : d_H(\mathbf{x}, \mathbf{y}) \leq r\}|$ le nombre de séquences de taille n dans une boule de centre $\mathbf{x}$ et de rayon r. Exprimer $V(\mathbf{x}, r)$ en fonction de n, q et r.

Question 2. Donner une borne sur le nombre de boules disjointes de rayon r.

Question 3. Montrer que si $\mathcal{C}$ est de distance d, alors tous ses mots de codes sont au centre de boules disjointes de rayon t.

Question 4. À l'aide des deux questions précédentes, montrer la borne de Hamming.

Exercice 7 - Code de Hamming

Le code de Hamming $[7, 4, 3]$ est un code linéaire dont la matrice de parité est la suivante :

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Question 1. Donner les paramètres k et n pour ce code.

Question 2. À l'aide de la matrice H, montrer qu'il existe un mot de code de poids 3.

Question 3. Montrer que la distance minimale de ce code est 3.

Question 4. Ce code est-il MDS ?

Question 5. Ce code est-il parfait ?